AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Subject Account	)	Case No. MJ20-021

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

The Subject Account as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 2252 (a)(2)	Receipt or Distribution of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

✓ See attached Affidavit continued on the attached sheet

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Toby G. Ledgerwood, Special Agent (HSI)

Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or

◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 01/17/2020

Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, Chief United States Magistrate Judge

Printed name and title

USAO: 2020R00035

ATTACHMENT A

Description of Property to be Searched

This warrant applies to information associated with the Apple iCloud account/email: slave524@icloud.com (the "account"), that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Photo Library, Photo Stream, iCloud Drive, Safari Browsing History, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) those violations occurring in or after September 2014, found in the Account listed on Attachment A, including the following:

a. Evidence of registration and use of Apple accounts, including communications sent via iMessage or FaceTime;

b. Evidence of registration;

c. Evidence of visual depictions of minors engaged in sexually explicit conduct;

d. Evidence that serves to identify any person who uses or accesses the Account or who exercises in any way any dominion or control over the Account;

e. Evidence that may reveal the current or past location of the individual or individuals using the Account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. Evidence of efforts to maintain anonymity online, including by accessing VPNs;

g. Other log records, including IP address captures, associated with the specified Accounts;

h. Subscriber records associated with the specified Accounts, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as IP address, media access card addresses, or any other unique device identifiers recorded by internet service provider in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

i. Records of communications between the internet service provider and any person purporting to be the account holder about issues relating to the Account, such as technical problems, billing inquiries, or complaints from other users about the specified Account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications;

j. iPhone identification number, MEID, IMSI, ICCID, and cellular telephone number;

k. Information identifying accounts that are linked or associated with the Accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, Inc. ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date:_____ Signature:_____

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF WHATCOM)

I, Toby Ledgerwood, being duly sworn on oath, depose and state:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), assigned to the Assistant Special Agent in Charge (ASAC) Blaine, Washington, field office. I have been employed as an HSI Special Agent since 2006. Prior to this assignment, I worked as a United States Customs Inspector from 2002 to 2006. In my capacity as a Special Agent, I am responsible for conducting investigations into the numerous federal laws enforced by HSI. Since 2013, I have investigated criminal violations relating to child exploitation and child pornography, including violations pertaining to the unlawful production, importation, distribution, receipt, attempted receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A(a). I am a graduate of the Federal Law Enforcement Training Center (FLETC), HSI Special Agent Training Program, and have received further specialized training in investigating child pornography and child exploitation crimes. My training included courses in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and the execution of search warrants. I have observed and reviewed thousands of examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have participated in the execution of many search warrants which involved child exploitation and/or child pornography offenses and the search and seizure of computers and other digital devices. Further, I have served as the affiant on numerous search warrants and complaints relating to child exploitation investigations. I am a member of the Internet

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children. I have attended periodic seminars, meetings, and training. I attended the ICAC Undercover Investigations Training Program in Alexandria, Virginia, in June 2014 regarding child exploitation. I also attended the Crimes Against Children Conference in Dallas, Texas, in August 2014, where I received training relating to child exploitation, including training in the Ares Peer to Peer (P2P) file sharing program. In September 2015, I received training in the Emule (P2P) file sharing program. I received a Bachelor of Science degree in Criminal Justice with a minor in Sociology from the University of Missouri-St. Louis.

2. I am submitting this affidavit in support of an application under for a search warrant for information associated with an account that is stored at premises controlled by Apple Inc. ("Apple"), located at One Apple Park Way in Cupertino, California, ("**THE PROVIDER**").

3. This affidavit is made in support of an application for a search warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **THE PROVIDER** to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachments B, pertaining to the following Apple iCloud account and email address:

slave524@icloud.com ("SUBJECT ACCOUNT")

user information of **iClouid account**:

Name: jon lakey

Address: 7317 elaine street

Blaine, WA 98230

Mobile Phone: 3605106600

4. Upon receipt of the information described in Section I of Attachments B, government-authorized persons will review that information to locate the items described

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

in Section II of Attachments B. This warrant is requested in connection with an on-going investigation in this district by Homeland Security Investigations.

5. The warrant would authorize a search of the **SUBJECT ACCOUNT**, for the purpose of identifying electronically stored data as particularly described in Attachment B, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography).

6. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

7. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), will be found in **SUBJECT ACCOUNT**.

8. This Affidavit is being presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

II. DEFINITIONS

9. The following definitions apply to this Affidavit:

Internet Service Providers

a. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "email address," an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP's servers.

Internet Protocol (IP) Addresses

b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer connected to the Internet must be assigned an IP address so that the Internet traffic sent from, and directed to, that computer may be properly directed from its source to its destination. Most ISPs control the range of IP addresses.

Apple ID

c. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. Apple uses a unique

Virtual Private Network (VPN)

d. A VPN connection is a means of connecting to a private network over a public network such as the Internet. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. VPN's are also frequently used by people who wish to circumvent geographic IP limitations and censorship, and to connect to proxy servers for the purpose of obfuscating the source of an internet connection or transmission.

III. The CyberTip and ESP Apple Inc

11. This investigation arose from a CyberTip submitted to the National Center for Missing and Exploited Children (NCMEC). NCMEC is a private non-profit organization operating under a Congressional mandate to act as the nation's law enforcement clearing house for information concerning online child sexual exploitation. In partial fulfillment of that mandate, NCMEC operates a CyberTip line, a resource for reporting online crimes against children. Electronic Service Providers (ESPs) report to NCMEC, via the CyberTip line, whenever they discover that a subscriber has violated the terms of service and/or their services have been used to transmit child pornography over the Internet.

12. The CyberTip giving rise to the instant investigation came from ESP Apple, Inc., an electronic communication/service provider and digital device manufacturer headquartered in Cupertino, California.

IV. STATEMENT OF PROBABLE CAUSE

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

13. In October 2019, Homeland Security Investigations (HSI) Blaine, Washington received CyberTip report #55619888 from the Seattle Internet Crimes Against Children (ICAC) Task Force. In the CyberTip, Apple reported one of its users, Jon Lakey, using email address slave524@icloud.com, uploaded several images of suspected child pornography from IP Address 172.98.86.39 (the SUBJECT IP ADDRESS) on September 17, 2019.

14. The uploads occurred in conjunction with attempts to send emails containing images of suspected child pornography from slave524@icloud.com to another email address. The CyberTip also indicated that this email contained the text "Sent from my iPhone," which is indicative of that email being sent using an Apple iPhone. However, an Apple representative confirmed in response to an inquire from me that Apple cannot definitively say whether or not the user of email address slave524@icloud.com was in fact using an iPhone at the time.

15. A query of a publicly available database revealed the SUBJECT IP ADDRESS belonged to ISP Total Server Solutions.

16. In response to an administrative summons seeking subscriber information for the SUBJECT IP ADDRESS at the time of the upload of suspected child pornography to Apple, Total Server Solutions responded with the following information: "Hello, We received your subpoena request. Total Server Solutions provides Infrastructure this client. This specific client would have a client on their end that was using the IP addresses provided in the subpoena. Hence, a subpoena directed towards them to retrieve that customer information would be needed. We are unsure of logs that our clients have as we just host their infrastructure within our data centers. We do not manage the actual applications on those servers. I have attached that information so you can proceed. If anything additional is required please let me know."

17. SA Ledgerwood reviewed the attachment, and the information provided indicated the SUBJECT IP ADDRESS belonged to Tefincom S.A. located in Panama City, Panama.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

18. On November 19, 2019, SA Ledgerwood sent a request for assistance to SA Harry Schmidt, HSI Panama. On November 20, 2019, SA Schmidt responded with the following; "appears that company is another server type company here in Panama. We have seen it before." "Send us the IP, dates, times, etc. that you want to look at and we will do a subpoena through Panama prosecutors and hopefully obtain the subscriber info." To date, there has been no further information provided by SA Schmidt.

19. From my training and experience, I believe it is likely the user of the SUBJECT ACCOUNT was using a VPN to access that account at the time Apple detected the attempted upload of child pornography to its servers. Thus, although the SUBJECT IP ADDRESS appears to be owned by a provider in Panama, I believe it is likely that the user of SUBJECT ACCOUNT is located in the Western District of Washington.

20. Included with the CyberTip was identifying information associated with the email address slave524@icloud.com, including the following:

Name: Jon Lakey

Address: 7317 Elaine Street, Blaine, Washington, 98230

Mobile Phone: 3605106600

21. The same Apple representative explained that the name, address, and phone number, were all provided by the user at the time of creation of the slave524@icloud.com account.

22. The Apple representative further explained, "I also went back and reviewed the actual emails. As I mentioned, we use hash matching on outgoing email. When we intercept the email with suspected images they do not go to the intended recipient. This individual [, slave524@icloud.com,] sent 8 emails that we intercepted. [Seven] of those emails contained 12 images. All 7 emails and images were the same as was the recipient email address. The other email contained 4 images which were different than the 12 previously mentioned. The intended recipient was the same. I suspect what happened was he was sending these images to himself and when they didn't deliver he sent them

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

again repeatedly. Either that or he got word from the recipient that they did not get delivered."

23. Before submitting the CyberTip, employee(s) of Apple Inc examined each of these images of suspected of child pornography.

24. I have reviewed these images as well, which Apple provided as part of the CyberTiP, and describe them below:

> **File 1**
> This color image depicts a prepubescent female (hereinafter the "child victim"). The child victim is nude and laying on her stomach facing the camera. The child victim is nude from the waist down except for her socks. An erect penis is seen in front of the child victim's face. The child victim appears to have a large amount of ejaculate on her face near her mouth and nose. The child victim is very small in stature and lacks muscular development. The child victim appears to be approximately 6 to 8 years old.
>
> **File 2**
> This color image depicts a prepubescent female (hereinafter the "child victim"). An adult male is nude laying on a bed with the child victim, who is also completely nude and sitting on top of the adult male. She is fully visible. The child victim's legs are spread apart and the male's erect penis is inserted into her vagina. The child victim's breasts are exposed. She lacks muscular and breast development, lacks visible pubic hair, and is very small in stature. The child victim appears to be approximately 8-10 years old.
>
> **File 3**
> This color image depicts a prepubescent female (hereinafter the "child victim"). The child victim is wearing black stockings, a pink collar, and hoop earrings. The child victim's breasts and genitals are exposed. An adult male's hairy, erect penis is seen being inserted or placed into the child victim's vagina. The child victim lacks muscular and breast development, lacks visible pubic hair, and is very small in stature. The child victim appears to be approximately 6-8 years old.

25. On November 5, 2019, at approximately 1200 hrs. Group Supervisor (GS) James Healy conducted surveillance of the SUBJECT PREMISES. It is a gray, single story residence with white trim bearing address "7317" in black numbers on white trim to the right of the door when facing the residence from the street. GS Healy took several photographs of the residence and saw children's toys in front of the residence on a table against the residence next to a black barbecue grill. Later, at approximately 1500 hrs,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

GS Healy saw two cars parked in the driveway of the residence, a white Acura passenger car bearing license plate WAUS/APX8330 and a light green Kia Soul SUV bearing license plate WAUS/BPA5152. At approximately 1520 hours GS Healy saw a balding white male, heavy set, with a long beard wearing black hoodie and pants leave the home walking a small dog and proceed south on Elaine St toward Bay Rd. That person appeared to be the same person shows on the Washington DOL photo associated with Jon Lakey (discussed below). At approximately 1535 hours GS Healy saw the same man return to the home accompanied by a minor male.

26. On November 6, 2019, GS Healy conducted a search via the Washington State Department of Licensing (WSDOL) and learned that Jon LAKEY has a 2007 Acura, registered at the SUBJECT PREMISES. WSDOL also revealed LAKEY was issued a Washington State driver's license on November 10, 2016, with the SUBJECT PRIMISES listed as his address. WSDOL also revealed the Jon LAKEY and R.K. have a 2013 Kia, registered at the SUBJECT PREMISES. WSDOL revealed R.K. was issued a Washington State driver's license on January 18, 2017, with the SUBJECT PREMISES listed as R.K.'s address.

27. Records checks conducted via the Whatcom County Assessor's Office revealed that Jon LAKEY and R.K. own the SUBJECT PREMISES. The SUBJECT PREMISES is listed on the Assessor's web-site as a doublewide manufactured home located on .17 acres. According to the Assessor's Office, they purchased the house in 2006.

28. On December 5, 2019, while conducting surveillance of the SUBJECT PREMISES, I used a portable electronic device to conduct a wireless survey from the public right of way adjacent to the SUBJECT PREMISES and discovered numerous Wi-Fi enabled networks. These Wi-Fi networks were all locked. During that survey, I also detected at least one "xfinitywifi" wireless internet network in the area. Based on my training and experience, I know that Comcast deployed a series of wireless "hotspot" networks for their customers. Comcast accomplished this by providing their wireless

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

internet customers with updated wireless routers capable of broadcasting an additional wireless network. These wireless "hotspot" networks are recognized by the connecting device as "xfinitywifi". Comcast customers can access "xfinitywifi" networks by logging in with their unique Comcast email or username and previously created password. Of particular importance is that the "xfinitywifi" networks are completely separate from the Comcast customer's private home wireless network(s). While conducting a prior investigation, an official with Comcast confirmed with me that Comcast's "xfinitywifi" wireless networks are not linked or connected to the Comcast subscriber's internet service.

29. A query of a publicly available database revealed the phone number 360-510-6600 belonged to ATT. In response to an administrative subpoena seeking subscriber information for that phone number, ATT provided the following information. The billing party for this number is R.K., and the billing address is the SUBJECT PREMISES. ATT reported that the user of the phone is Jon Lakey and that service between in 2004 and was current as of December 2019. The contact email for that user was listed as SLAVE524@HOTMAIL.COM.

30. As outlined above, multiple sources of information indicate that LAKEY, currently resides at the SUBJECT PREMISES and resided there on the dates that child pornography files were uploaded from the SUBJECT IP ADDRESS via LAKEY's email. I believe that LAKEY used likely a mobile device to distribute child pornography via the Internet, and that evidence of that crime will be found in the **SUBJECT ACCOUNT**.

IV. BACKGROUND CONCERNING ONLINE ACCOUNTS

31. As explained herein, information stored in connection with an online account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

32. In my training and experience, the information stored in connection with an online account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time.

33. Further, information maintained by the online provider can show how and when and where the account was accessed or used. For example, as described below, online providers typically log the Internet Protocol (IP) addresses from which users access an account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email).

34. Stored electronic data may provide relevant insight into the online account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

Apple's Services

35. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

36. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

37. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

38. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps. iCloud can be utilized to transfer data from an old device to a new device, including data derived from device backups and third-party applications.

39. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

40. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

41. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

42. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

43. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

44. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

45. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

46. In this case, I am investigating, among other things, the use of an Apple account to distribute child pornography. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. Stored e-mails, chats, and other files may not only contain communications relating to the crimes under investigation, but also help identify the participants in those crimes. Address books and contact lists may help identify and locate the distributor, or those associated with him/her. Search and browsing history may also constitute direct evidence of the crimes under investigation to the extent the browsing history or search history might include searches and browsing history and other evidence of the crimes under investigation or indications of the true identity of the account user. In my training and experience, I also know that the commission of the violations in the manner set forth above necessarily requires the use of computers, smart phones, tablets, or other computer devices.

47. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

48. Other information connected to an Apple ID may lead to the discovery of additional evidence. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of the distibutor and instrumentalities of the crimes under investigation. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services.

V. PERSONS WITH A SEXUALIZED INTEREST IN CHILDREN AND DEPICTIONS OF CHILDREN

49. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly. They also may opt to store the contraband in cloud accounts. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage can span multiple servers, and often locations, and the physical environment is typically owned and managed by a hosting company. Cloud storage allows the offender ready access to the material from any device that has an Internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender's device.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. E-mail itself provides a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

stored on email "cloud" servers, which allow users to store a large amount of material at no cost, without leaving any physical evidence on the users' computer(s).

50. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

51. Given the above-stated facts, including the circumstances surrounding the Apple Inc CyberTip and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that the iClouid account/email slave524@icloud.com user likely has a sexualized interest in children and depictions of children. I therefore believe that evidence of child pornography is likely to be found in the **SUBJECT ACCOUNT**.

VI. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

52. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to require **THE PROVIDERS**, and their agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to **THE PROVIDERS** with direction that they

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

identify the accounts described in Attachments A to this affidavit, as well as other subscriber and log records associated with the accounts, as set forth in Section I of Attachments B to this affidavit.

53. The search warrant will direct **THE PROVIDERS** to create an exact copy of the specified account and records.

54. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data and identify from among that content those items that come within the items identified in Section II to Attachments B for seizure.

55. Analyzing the data contained in the forensic copy may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common email, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachments B to the warrant.

56. Based on my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize a variety of e-mail communications, chat logs and documents, that identify any users of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

subject account and e-mails sent or received in temporal proximity to incriminating e-mails that provide context to the incriminating communications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

VII. CONCLUSION

57. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are located in the **SUBJECT ACCOUNT** as more fully described in Attachment A to this Affidavit. I therefore request that the court issue a warrant authorizing a search of the **SUBJECT ACCOUNT** specified in Attachment A for the items more fully described in Attachment B.

Toby Ledgerwood, Affiant
Special Agent
Department of Homeland Security
Homeland Security Investigations

The above named agent provided a sworn statement attesting to the truth of the forgoing affidavit this 17 day of January, 2020.

BRIAN A. TSUCHIDA
Chief United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Description of Property to be Searched

This warrant applies to information associated with the Apple iCloud account/email: slave524@icloud.com (the "account"), that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Photo Library, Photo Stream, iCloud Drive, Safari Browsing History, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) those violations occurring in or after September 2014, found in the Account listed on Attachment A, including the following:

a. Evidence of registration and use of Apple accounts, including communications sent via iMessage or FaceTime;

b. Evidence of registration;

c. Evidence of visual depictions of minors engaged in sexually explicit conduct;

d. Evidence that serves to identify any person who uses or accesses the Account or who exercises in any way any dominion or control over the Account;

e. Evidence that may reveal the current or past location of the individual or individuals using the Account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. Evidence of efforts to maintain anonymity online, including by accessing VPNs;

g. Other log records, including IP address captures, associated with the specified Accounts;

h. Subscriber records associated with the specified Accounts, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as IP address, media access card addresses, or any other unique device identifiers recorded by internet service provider in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

i. Records of communications between the internet service provider and any person purporting to be the account holder about issues relating to the Account, such as technical problems, billing inquiries, or complaints from other users about the specified Account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications;

j. iPhone identification number, MEID, IMSI, ICCID, and cellular telephone number;

k. Information identifying accounts that are linked or associated with the Accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, Inc. ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date:_____ Signature:_____

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970